

interview questions which Defendant answered: Defendant confirmed his identity, gave his address, date of birth, why he was in Charlotte, whether he had a cell phone, and what his cell phone number is.

After law enforcement asked Defendant the series of questions, they informed him he was under arrest, and read him his Miranda rights. Law enforcement then asked Defendant whether he was willing to discuss the matter further. Defendant said no and the interview ended without further questioning.

b. Cell Phone Was Searched

After the cell phones were seized, law enforcement applied for and were granted a search warrant to search the cell phones. The cell phone at issue here was password protected. Law enforcement used software to bypass the passcode and gain entry to the phone. Specifically, the phone was searched by a detective with the Charlotte Mecklenburg Police Department Cyber Crime and Digital Forensics Unit, who used forensic software from a private company to bypass the phone's password "lock" to access the phone's contents. As a result of the search, data and other information incriminating Defendant were obtained.

II. Discussion

Defendant has filed two motion to suppress. First, Defendant wishes to suppress his statement about his cell phone number and resulting evidence. (Doc. No. 53). Second, Defendant wishes to suppress the data and information obtained through law enforcement's search of the cell phone. (Doc. No. 54). The Court will address these motions ad seriatim.

a. Suppression of Defendant's Statement About His Cell Phone Number is Moot

The Fifth Amendment guarantees that “[n]o person...shall be compelled in any criminal case to be a witness against himself, nor be deprived of life, liberty, or property, without due process of law ...” U.S. Const. amend. V. In Miranda v. Arizona, the Supreme Court recognized that custodial interrogation by the police is inherently coercive, and consequently held that detailed warnings were required to protect the privilege against compulsory self-incrimination. 384 U.S. 436, 444 (1966). Accordingly, Miranda warnings must be administered to a person prior to custodial interrogation. However, there is an exception. The “booking exception” permits law enforcement to obtain basic personal information such as an individual’s name, age, and place of birth without reading a Miranda warning, as those questions do not constitute interrogation. United States v. Taylor, 799 F.2d 126, 128 (4th Cir. 1986). However, the police may not ask questions, even during booking, that are designed to illicit incriminatory admissions. Id. (quoting United States v. Morow, 731 F.2d 233, 237 (4th Cir. 1984)).

Here, Defendant argues that law enforcement’s request of his cell phone number, before he was read his Miranda rights, was designed to illicit an incriminatory admission and therefore does not fall within the booking exception. The Government responds that the request for Defendant’s cell phone number falls within the booking exception. The Government further contends that even if a Miranda violation occurred when law enforcement asked Defendant to provide his phone number, the contents of the cell phone are not excludable as “fruits of the poisonous tree.” Lastly, the Government requests the Court to find the issue moot, since the Government has agreed not to admit evidence in its case-in-chief that Defendant provided a cell phone number, what that number was, or that Defendant answered any law enforcement questions about a cell phone.

Because the Government has agreed not to use evidence that Defendant provided a cell phone number, what that number was, and that Defendant answered any law enforcement questions about a cell phone as part of its case-in-chief, it appears the issue of suppressing Defendant's statement about his cell phone number is moot. United States v. Holcomb, No. 1:20 CR 78 MR WCM, 2020 WL 7647788, at *1 (W.D.N.C. Dec. 4, 2020), report and recommendation adopted, No. 1:20-CR-00078-MR-WCM, 2020 WL 7646810 (W.D.N.C. Dec. 23, 2020) (finding Defendant's motion to suppress an out-of-court identification moot because the Government consented not to use such evidence in its case-in-chief).

Defendant argues that his provision of his cell phone number led to the search of the cell phone at issue in this case, and therefore the information obtained through the search of the cell phone should be suppressed as well. However, Defendant has not shown a connection between Defendant's provision of his cell phone number and the search warrant that authorized the search of the cell phone at issue in this case. Nix v. Williams, 467 U.S. 431, 448 (1984) ("But when, as here, the evidence in question would inevitably have been discovered without reference to the police error or misconduct, there is no nexus sufficient to provide a taint and the evidence is admissible."). Indeed, the warrant application does not contain any mention of the phone number Defendant provided or the fact that Defendant discussed any phone number with law enforcement. The affidavit of Detective Hagler accompanying the warrant did not contain any mention of the phone number Defendant provided or the fact that Defendant discussed any phone number with law enforcement. And the Search Warrant itself did not contain any mention of the phone number Defendant provided or the fact that Defendant discussed any phone number with law enforcement.

Because the suppression of Defendant's statement is moot and there is no factual nexus connecting Defendant's statement to resulting evidence, Defendant's motion to suppress his statement about his cell phone number and resulting evidence is denied.

b. The Government did not Exceed the Scope of its Search Warrant when it used Software to Access the Cell Phone

If the scope of a search exceeds what is permitted by the terms of a validly issued warrant, the search and any subsequent seizure are unconstitutional. Horton v. California, 496 U.S. 128, 140 (1990). Defendant argues that a Court must look at the text of the warrant itself, not the application for a warrant, when deciding whether a search exceeds the scope of a warrant. The cell phone search warrant permitted law enforcement to search the phone, but it did not provide permission to use an outside company's software to forcibly enter the phone. According to Defendant, because the search warrant lacks particularity as to the required forced entry, that forced entry qualifies as a search that exceeded the scope of the search warrant. The Government argues that a search warrant need not describe the precise means by which a search is executed; it need only be particular about what is being searched and seized – and here the warrant described what was to be searched and seized with sufficient particularity.

As an initial matter, it is unclear whether Defendant has standing to challenge a search of the cell phone in question. To challenge a search under the Fourth Amendment, a defendant must have "a reasonable expectation of privacy" in the place that was searched. Rakas v. Illinois, 439 U.S. 128, 143 (1978). Here, the place searched was a cell phone. Defendant has not conceded the cell phone belongs to him or that he has any other expectation of privacy in the cell phone or its contents. Accordingly, Defendant lacks standing to raise a claim that the search of a cell phone that does not belong to him violates his Fourth Amendment rights. Plumhoff v. Rickard, 572

U.S. 765, 778 (2014) (“Fourth Amendment rights are personal rights which ... may not be vicariously asserted.”) (quoting Alderman v. United States, 394 U.S. 165, 174 (1969)); See also, United States v. DiTomasso, 56 F. Supp. 3d 584, 590 (S.D.N.Y. 2014) (“A person lacks standing to raise Fourth Amendment claims if the disputed evidence was procured by a search of a third person's premises or property rather than his own premises or property.”) (internal citations and quotations omitted).

Even if Defendant were to state the cell phone belongs to him, his Motion to Suppress would be denied, because law enforcement did not exceed the scope of its judicially-authorized search when it used forensic software to bypass the cell phone’s passcode and gain entry to its contents. The Fourth Amendment “specifies only two matters that must be ‘particularly described’ in the warrant: ‘the place to be searched’ and ‘the persons or things to be seized.’” United States v. Grubbs, 547 U.S. 90, 97 (2006). See also United States v. Blakeney, 949 F.3d 851, 862 (4th Cir. 2020) (“So long as the warrant describes the items to be seized with enough specificity that the executing officer is able to distinguish between those items which are to be seized and those that are not ... the particularity standard is met.”) (internal citations and quotations omitted). A search warrant need not specify the precise method or methods used for executing a search warrant. Here, the search warrant identified the place to be search—the cell phone—and law enforcement appropriately limited their search to that place. Furthermore, law enforcement did not utilize unreasonable or destructive methods in executing the search warrant. Therefore, law enforcement acted within the scope of its judicially-authorized search.

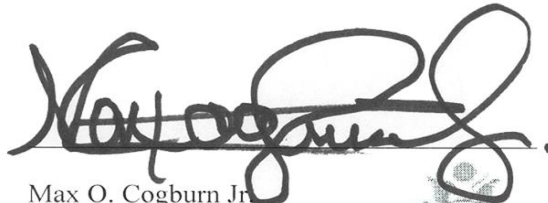
III. Conclusion

Having carefully considered Defendant's Motions to Suppress, the memoranda submitted, and heard the evidence presented, the Court enters the following Order denying the two motions to suppress.

ORDER

IT IS, THEREFORE, ORDERED that Defendant's Motions to Suppress, (Doc. Nos. 53, 54), are **DENIED**.

Signed: February 1, 2023



Max O. Cogburn Jr.
United States District Judge